NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

Formerly known as *Critical Infrastructure Developments*

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.

Issue 3-01
March 23, 2001

Editors: Linda Garrison
Martin Grand

- **Healthcare: Access to Medical Information Files Requires Enhanced Security**
- **Theft of Distributed Computing Power: A Popular Attack Motive**
- **Virus Technology: Increasing Use of Personal Digital Assistants Creates New Security Concerns**
- **What's new at the NIPC**

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or call (202)323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, please participate in our reader survey, or contact the Editors at (202) 324-0334 or (202) 324-0353. A reader survey form is attached.

Healthcare: Access to Medical Information Files Requires Enhanced Security

Concerns surrounding information security in the healthcare industry mirror concerns experienced in other sectors that have implemented networked information systems.

U.S. healthcare institutions have much to gain from the wide spread implementation of the electronic knowledge management tools and inter-networked information systems that are transforming other sectors of our economy. If detailed and comprehensive records such as individual and family medical histories, medical test results, current medications, and patient status information become available electronically, instantaneous remote access to this information will transform the state-of-the-art of healthcare delivery.

For example, emergency healthcare providers could access their patients' complete medical files while transmitting real-time patient status information back to a fully equipped healthcare facility for evaluation by specialists. While the trend toward remote electronic access to networked medical records offers many advantages, it also makes individual patient information vulnerable to a wide range of malicious activity.

Confidentiality is particularly important for medical records due to the sensitive personal nature of the information. Patient records are also often tied to billing information. Those medical records usually contain a patient's Social Security Number, date of birth, physical description, and other information that could be used to perpetrate identity theft or other types of fraud. Data integrity is another aspect, as even minor modifications to patient information could have tragic results for the individual under treatment. In some applications, the availability of timely data may be another important criterion for information systems in the healthcare industry.

Over the past months, there have been a number of incidents indicating that the development of information security in the healthcare industry parallels the issues that have been observed in other information-dependent sectors of the economy.

- Healthcare professionals have discovered the convenience of using e-mail to communicate with patients. However, medical professional organizations have expressed concern about doctors using unsecured e-mail to communicate potentially sensitive information, noting that there are no mechanisms to control the distribution or storage of the data being transmitted. In one incident, e-mail messages with patient data were sent to the wrong person. Other media accounts related instances in which computer system administrators intercepted and read confidential information sent to patients via e-mail.

- In the fall of 1999, the publisher of a web-site associated with the computer underground informed the media of a security problem with a telephone-based patient data system at a U.S. hospital. The hospital used a digital dictating system that allowed doctors to dictate notes about patients or to listen to previously recorded patient records. The problem stemmed from the fact that anyone could dial in to the hospital's telephone system and listen to the records of any patient in the

database. As proof, an audio file consisting of a patient record from the database was posted on the Internet.

- National media reported a more traditional computer breach when a hacker broke into the computer systems of a hospital at a large American university and copied electronic files containing records on thousands of patients. As proof of the access, the European-based hacker provided copies of some patient records to at least one journalist.

The healthcare industry, through professional and industry organizations, is actively examining issues surrounding data privacy and security. Specialists are working on implementing improvements in information security regimes. The U.S. Department of Health and Human Services is also developing a comprehensive package of guidelines designed to aid healthcare organizations in improving their information security programs.

Complete and unrestricted access to detailed patient records by healthcare providers will enable substantive leaps in the quality of medical treatment. However, damage can be done if the integrity, availability or confidentiality of this sensitive information is compromised. Efforts are underway to ensure that the industry develops and implements secure, workable, and commercially viable solutions to these challenges.

Theft of Distributed Computing Power: A Popular Attack Motive

Security managers contend with a wide array of malicious activities perpetrated against end users by mobile malware. An esoteric type of emerging threat is malware that steals a user's computer processing power to work on a complex computational problem of the attacker's choosing.

Theft of computing power typically involves the unauthorized distribution and installation of otherwise harmless software utilized in one of the numerous distributed computing projects active on the Internet. Distributed computing projects seek to utilize the combined computing power of thousands of volunteers to solve particularly complex mathematical or scientific problems. Participants install a small client program on their computer that downloads and processes a small portion of a complex computing task. When one part has been completed, the client automatically uploads the results to a central server and retrieves a new portion of the task to process.

One such distributed computing project, Distributed.net, attempts to crack encrypted messages in response to challenges issued by security vendors. This effort is structured as a contest with the amount of computing power each participant has contributed to the overall project credited to an account matched to his e-mail address. Security concerns around this project arose from its inception. In 1997, the group warned that malicious actors had trojanized versions of selected shareware installation programs available on the Internet so that the Distributed.net client would be installed along with other software. In 2000, it also warned that researchers had found some variants of the VBS.Network and QAZ.Trojan worms that installed versions of the Distributed.net client on victims' computers.

The Bymer worm, which appeared in the wild in October 2000, may also be referenced under such names as Dnet.Dropper, MSINIT, WININIT, or Worm.RC5, has been found in at least two major variants. It appears to have been specifically designed and crafted to surreptitiously install the Distributed.net client software on victims' computers while arranging to have the results of their computing efforts credited to the attacker's account. This worm propagates on the Microsoft Windows platform via shared network drives. Generally speaking, Bymer scans random IP addresses looking for an available share named "C" and a folder called "Windows." If it finds one, it copies itself along with the files dnetc.exe and dnetc.ini—files utilized in the Distributed.net project to the target computer. It also modifies the computer's system files to ensure that the worm and the Distributed.net client will be run during all subsequent Windows sessions.

In 1998, a telecommunications company's computer staff was called to investigate a serious network slowdown. The computers, which would normally respond to a query in a few seconds, were taking up to five minutes to respond. At times network response was reportedly so poor that customer telephone calls were re-routed to other states. Staff eventually discovered an extra software program running on thousands of company workstations. This program was traced back to a contract computer consultant working at a facility in Colorado. The perpetrator, a self-professed "math geek," admitted that he had been participating in an Internet-based distributed computing effort known as the Great Internet

Mersenne Prime Search (GIMPS). As part of his quest to find a new prime number, he had remotely installed the GIMPS client program on computers throughout the network.

The victim company estimated that by running the program on some 2,500 company workstations, the contractor had hijacked 10.63 years of computer processing time. According to one report, he had misconfigured the client software to check for updates far more often than it normally would have, leading to severe degradation in performance of the company's far-flung network and eventually, to the discovery of the unauthorized use of the company's computers.

Distributed computing is a technology trend that may well continue to develop in the future. The potential computational power offered by millions of otherwise idle computers is too impressive to ignore. However, as with any other new application of networking technology, the possibility for malicious abuse exists. The incidents described above serve to remind network managers that there are ways to attack and misuse computing resources, which they may have not even imagined.

Virus Technology: Increasing Use of Personal Digital Assistants Creates New Security Concerns

Personal Digital Assistants (PDAs) may serve as conduits for the introduction of malicious software (malware) into enterprise networks.

In today=s information-driven world, PDAs have become seemingly ubiquitous. Personal schedules, contact information, reminders, and other personal applications such as accessing the web can be kept on a device the size of a wallet. The market research firm International Data Corporation (IDC) has estimated that 12.9 million smart handheld devices were shipped last year, and the market is steadily growing.

PDAs have attracted the attention of authors of malware. In the fall of 2000, two pieces of malware appeared which attacked devices running the Palm OS. The Liberty Trojan horse, which was disseminated on the Internet, deleted executable applications from the PDA on which it was loaded and run. A few weeks later, Palm OS users were confronted with the threat posed by the Phage virus, which could be spread when the device=s data was backed up to a user=s personal computer or when the PDA exchanged data with another device also running the Palm OS. While viruses specifically targeting PDAs are presently rare, malware could emerge as a serious concern as the popularity of these devices increase.

Another virus threat involves the interaction between PDAs and personal computers (PCs) in networked environments. Like any other business asset, the information on PDAs must be protected. A number of applications exist that enable users to "synchronize" or compare and standardize information from PDAs to PCs as well as to exchange data between users. It has been estimated that 80 percent of handheld devices are being periodically synchronized in a work environment. With the emergence of PDA-based viruses, it could be possible to inadvertently share malicious code with other users.

In one potential scenario, a PC-based worm (a stand-alone program that replicates itself on one computer and attempts to infect all other computers connected to that network) could insert a PDA-based virus into the directory structure allocated for synchronizing data to handheld devices, causing the virus to be downloaded to PDAs during each device=s next synchronization. This virus could execute attacks ranging from erasing all the PDA=s data to siphoning data back to the PC-based worm for further exploitation by the attacker.

The speed with which PDAs have become a standard business tool caught many information technology policy makers by surprise. Corporate security policy should consider protocols for the prevention, detection, and eradication of any malicious code introduced to their networks through a PDA. Virus concerns surrounding handheld computing devices will become even more pressing as these devices become increasingly used in a networked environment.

What's new at the NIPC -

InfraGard

The NIPC introduced the National InfraGard Program to the public on 5 January 2001. InfraGard began as a pilot project in 1996 by the Cleveland FBI Field Office and is a government and law enforcement alliance with the private sector. Local computer professionals assist the FBI in determining how to better protect critical information systems in the public and private sectors. From this new partnership, the first InfraGard Chapter was formed to address both cyber and physical threats. Today, all 56 field offices of the FBI have opened an InfraGard chapter, with a total of 518 company members across the U.S. InfraGard provides formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities.

InfraGard is needed because most infrastructure components are privately owned and operated, are often interconnected, have an increased reliance on automation, and are increasingly vulnerable to harm as the globalization of infrastructures progresses.

Janet Reno, the former Attorney General, has previously stated, "The InfraGard Program allows law enforcement and industry to work together and share information regularly, including information that could prevent potential intrusions into our national infrastructure. Building bridges between law enforcement and the public and private sector is one of the most important ways we can protect ourselves from these threats."

InfraGard addresses threats from insiders, hackers, organized crime, industrial espionage, terrorists, intelligence agencies and information warriors.

Additional information on this initiative can be obtained on the World Wide Web at <**www.nipc.gov**>.

Questionnaire

HIGHLIGHTS
March 23, 2001, Issue 3

In order to provide a service which is relevant to our clients, we would like your opinions on this publication. Please execute this questionnaire and return to the address at the bottom.

Please circle the most appropriate response:

1. Highlights presents issues which are_____ to my concerns.
not relevant / relevant

2. The information is presented in a _____ fashion.
jumbled / clear and understandable / too technical

3. The quality of the information presented is _____.
low / adequate / high

4. The frequency of the publication is _____.
too seldom / adequate / too frequent

5. I find the length of the articles to be
_____.
too short / appropriate / too long

6. Past articles have been informative. Yes No

7. What kind of articles would you find helpful in the performance of your duties?
_____
_____
_____

8. Overall assessment.
_____
_____
_____

What is your job title? _____
Would you like to contribute an article? If so, what would the topic be? Yes or No
Thank you for your time.
Please return this form to: Editor's, Highlights
Room 11719, NIPC, Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W., Washington, D.C. 20535

Fax: (202)324-0311

or E-mail - lgarrison@fbi.gov or mgrand@fbi.gov